(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－269524
（P2002－269524A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　19/077		Ｂ４２Ｄ　15/10	５２１	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｇ０６Ｋ　19/00	Ｋ	５Ｂ０３５
Ｇ０６Ｋ　19/073			Ｐ	

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願2001－67248(P2001－67248)

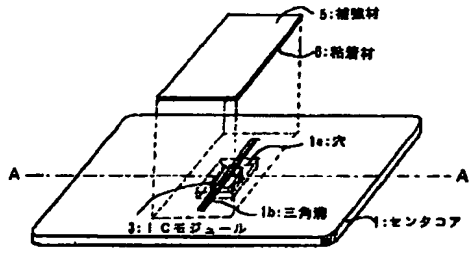
(22)出願日　平成13年３月９日(2001.3.9)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　宇佐見　慎一
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100086807
弁理士　柿本　恭成

Ｆターム(参考)　2C005 MA03 MA27 MA34 MB01 PA27 QC04 RA12 SA03
5B035 AA13 BA03 BB09 CA01 CA38

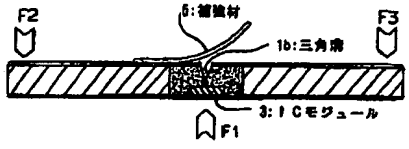
(54)【発明の名称】　ＩＣカード

(57)【要約】
【課題】　廃棄時に容易にセキュリティを確保できるＩＣカードを提供する。
【解決手段】　プラスチック製のセンタコア１に空けられた穴１ａの内部に、ＩＣモジュール３が封止樹脂４で埋め込まれたＩＣカードにおいて、このＩＣモジュール３の埋め込み箇所に対応するカード表面に、所定の深さの三角溝１ｂを設け、この三角溝１ｂを覆うように補強材５を粘着材６で貼り付ける。これにより、ＩＣカードは通常の強度を保つことができる。廃棄時には、補強材５を剥がし、三角溝１ｂの下側から指等で力Ｆ１を加えると共に、カードの両端に逆方向の力Ｆ２，Ｆ３を加える。これにより、三角溝１ｂの箇所でＩＣモジュール３が確実に破壊され、このＩＣモジュール３に記憶された情報を読み出すことができなくなる。



（ａ）外観

（ｂ）Ａ－Ａ断面



（ｃ）廃棄方法

本発明の第１の実施形態のＩＣカード

1

【特許請求の範囲】

【請求項１】　プラスチック製のカードにＩＣモジュールを埋め込んで形成されたＩＣカードにおいて、
前記ＩＣモジュールの埋め込み箇所に対応するカード表面に所定の深さの溝を設けると共に、該溝を覆うように該カード表面に補強材を非硬化性の粘着材で貼り付けたことを特徴とするＩＣカード。

【請求項２】　入力された情報を予め組み込まれたプログラムに従って処理する機能部と、
前記機能部の処理結果を格納する不揮発性の記憶部と、導電性塗料で形成された固有の配線パターンに従って暗号キーを発生するコード発生部と、
前記機能部から出力された処理結果のデータを前記暗号キーに従って暗号化して前記記憶部に書き込む共に、該記憶部から読み出されたデータを該暗号キーに従って復号化して該機能部に与える暗号部と、
前記機能部、記憶部、コード発生部及び暗号部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、
前記カードの窓部を覆う蓋とを、
備えたことを特徴とするＩＣカード。

【請求項３】　導電性塗料で形成された固有の配線パターンに従って固有コードを発生するコード発生部と、
予め設定された識別コードと前記固有コードが一致したときに動作許可信号を出力する一致検出部と、
前記動作許可信号が与えられたときに、入力された情報を予め組み込まれたプログラムに従って処理する機能部と、
前記コード発生部、一致検出部及び機能部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、
前記カードの窓部を覆う蓋とを、
備えたことを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣ（集積回路）カード、特に廃棄時に記憶情報を読めなくしてセキュリティを確保する技術に関するものである。

【０００２】

【従来の技術】ＩＣカードに個人情報等の機密性の高い情報を記録して利用する場合、そのカードが不要になったときにそのまま廃棄すると、そこに記録されている情報が漏洩して問題となるおそれがある。そのため、ＩＣカードの廃棄時には、そこに記録されている情報を確実に読み出せなくする必要がある。

【０００３】従来、ＩＣカードに記録された情報を読み出せなくする方法としては、専用の装置によって情報を電気的に消去する方法、専用の機械によってＩＣカードを物理的に破壊する方法、使用者がはさみ等の一般的な道具で破壊する方法等が採られていた。

2

【０００４】

【発明が解決しようとする課題】しかしながら、従来のように、何らかの装置、機械または道具が必要であると、使用者が何時でも処置を行えるとは限らないので、使用者の怠慢等により廃棄時の適切な処置が徹底されないおそれが多い。

【０００５】また、専用の装置で情報を消去した場合でも、確実に消去されたか否かを目視で確認できないので、廃棄時に感情的に不安が残る。また、はさみ等の道具で破壊した場合でも、ＩＣチップ部分が破壊されずにそのまま残っていると、情報が漏洩するおそれがある。

【０００６】本発明は、前記従来技術が持っていた課題を解決し、廃棄時に道具等を使用せずに、容易に記録情報を読み出せなくしてセキュリティを確保できるＩＣカードを提供するものである。

【０００７】

【課題を解決するための手段】前記課題を解決するために、本発明の内の第１の発明は、プラスチック製のカードにＩＣモジュールを埋め込んで形成されたＩＣカードにおいて、前記ＩＣモジュールの埋め込み箇所に対応するカード表面に所定の深さの溝を設けると共に、該溝を覆うように該カード表面に補強材を非硬化性の粘着材で貼り付けている。

【０００８】第１の発明によれば、以上のようにＩＣカードを構成したので、このＩＣカードを廃棄する場合、カード表面の補強材を剥がし、このカード表面に設けられた溝の部分で折り曲げれば良い。これにより、溝の部分において埋め込まれたＩＣモジュールが破壊され、このＩＣモジュール内に格納された情報を読み出すことができなくなり、セキュリティを確保することができる。

【０００９】第２の発明は、ＩＣカードにおいて、入力された情報を予め組み込まれたプログラムに従って処理する機能部と、前記機能部の処理結果を格納する不揮発性の記憶部と、導電性塗料で形成された固有の配線パターンに従って暗号キーを発生するコード発生部と、前記機能部から出力された処理結果のデータを前記暗号キーに従って暗号化して前記記憶部に書き込む共に、該記憶部から読み出されたデータを該暗号キーに従って復号化して該機能部に与える暗号部と、前記機能部、記憶部、コード発生部及び暗号部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、前記カードの窓部を覆う蓋とを備えている。

【００１０】第２の発明によれば、このＩＣカードを廃棄する場合、窓部の蓋を取り外して、コード発生部の導電性塗料による固有の配線パターンを削り取れば良い。これにより、暗号部に与えられる暗号キーが変更され、変更前の暗号キーで暗号化されて記憶部に書き込まれているデータを正しく読み出すことができなくなる。

【００１１】第３の発明は、ＩＣカードにおいて、導電

性塗料で形成された固有の配線パターンに従って固有コードを発生するコード発生部と、予め設定された識別コードと前記固有コードが一致したときに動作許可信号を出力する一致検出部と、前記動作許可信号が与えられたときに、入力された情報を予め組み込まれたプログラムに従って処理する機能部と、前記コード発生部、一致検出部及び機能部を埋め込むと共に、該コード発生部の配線パターンを露出させる窓部を有するプラスチック製のカードと、前記カードの窓部を覆う蓋とを備えている。

【００１２】第３の発明によれば、このＩＣカードを廃棄する場合、窓部の蓋を取り外して、コード発生部の導電性塗料による固有の配線パターンを削り取れば良い。これにより、一致検出部に与えられる固有コードが変更され、予め設定されている識別コードに一致しなくなるので、機能部の動作が不可能になり、他人に使用されるおそれがなくなる。

【００１３】

【発明の実施の形態】（第１の実施形態）図１（ａ）～（ｃ）は、本発明の第１の実施形態を示すＩＣカードの概略の構成図であり、同図（ａ）は外観を示す組立図、同図（ｂ）は同図（ａ）におけるＡ－Ａ断面図、及び同図（ｃ）は廃棄方法を示す説明図である。

【００１４】このＩＣカードは、図１（ａ），（ｂ）に示すように、縦５４ｍｍ、横８６ｍｍ、厚さ０．５ｍｍ程度の、硬質塩化ビニール等のプラスチックを材料とするセンタコア（中心部材）１の両面を、同様のプラスチックによるオーバーシート２Ａ，２Ｂでサンドイッチ状に挟んで、一体化した構造となっている。標準的なＩＣカードの全体の厚さは、０．７６ｍｍ程度である。

【００１５】センタコア１の所定の位置には、ＩＣモジュール３を収納するための穴１ａが設けられており、オーバーシート２AにこのＩＣモジュール３が接着されている。穴１ａには、ＩＣモジュール３を保護すると共にカードの強度を維持するために、封止樹脂４が充填されている。

【００１６】更に、ＩＣカードの中央部の表面には、ＩＣモジュール３の上部を通るように、縦方向に直線状の三角溝１ｂが設けられている。三角溝１ｂの深さは、オーバーシート２Ｂを越えて封止樹脂４及びセンタコア１の一部まで達するが、ＩＣモジュール３には届かない程度に形成されている。三角溝１ｂの表面には、硬質塩化ビニール板等の補強材５が非硬化性の粘着材６で貼り付けられている。

【００１７】このようなＩＣカードは、例えば、次のような工程で製造される。まず、ＩＣモジュール３を収納するための穴１ａを空けたセンタコア１の一方の面に、オーバーシート２Ａを熱接着し、この穴１ａの底部にＩＣモジュール３を接着剤で固定した後、その上に封止樹脂４を注入して硬化させる。更に、センタコア１の他の面にオーバーシート２Ｂを熱接着する。ここまでは、従来通りのＩＣカードの製造工程である。

【００１８】次に、カッター等を使用して、ＩＣカードの縦方向に一定の長さと深さを有する三角溝１ｂを形成する。このとき、三角溝１ｂは、オーバーシート２Ｂの上から、ＩＣモジュール３の上部を通り、このＩＣモジュール３に達しないような深さに形成する。

【００１９】更に、三角溝１ｂを覆うように、オーバーシート２Ｂの表面に補強材５を非硬化性の粘着材６で貼り付ける。これによって、本実施形態のＩＣカードが完成する。

【００２０】このようなＩＣカードは、オーバーシート２Ｂの表面に補強材５が貼り付けられた状態で使用される。これにより、三角溝１ｂによる強度的な弱点箇所が補強材５で補強され、通常の強度を保つことができる。

【００２１】一方、このＩＣカードを廃棄する場合には、図１（ｃ）に示すように、オーバーシート２Ｂの表面から補強材５を剥がし、三角溝１ｂの下側から指等で上向きに力Ｆ１を加えると共に、ＩＣカードの両端に下向きの力Ｆ２，Ｆ３を加える。これにより、ＩＣカードは三角溝１ｂの箇所で折り曲げられ、ＩＣモジュール３が完全に破壊される。

【００２２】以上のように、この第１の実施形態のＩＣカードは、ＩＣモジュール３の上部に折り曲げ用の三角溝１ｂを有するので、道具を使用せずにＩＣモジュール３を完全に破壊することができる。従って、廃棄時に記録情報を読み出せなくしてセキュリティを確保できる。また、ＩＣモジュール３が破壊されたことを、目視または手触り等で確認することができるので、安心してＩＣカードを廃棄することができるという利点がある。

【００２３】（第２の実施形態）図２（ａ）～（ｃ）は、本発明の第２の実施形態を示すＩＣカードの概略の構成図であり、同図（ａ）は外観を示す組立図、同図（ｂ）は同図（ａ）におけるＢ－Ｂ断面図、及び同図（ｃ）はコード発生部の平面図である。

【００２４】このＩＣカードは、図２（ａ），（ｂ）に示すように、縦５４ｍｍ、横８６ｍｍ、厚さ０．７６ｍｍ程度の、硬質塩化ビニール等のプラスチックを材料とするＩＣカード本体１０の内部に、コード発生部２０、信号線群３０及びＩＣモジュール４０を埋め込んだ構造となっている。コード発生部２０の上部には、窓部１１が開口され、この窓部１１が蓋１２で塞がれている。蓋１２の周囲は、非硬化性の粘着材で封止され、使用中に蓋１２が外れたり、隙間からごみや湿気等が侵入しないようになっている。

【００２５】コード発生部２０は図２（ｃ）に示すように、基板２１上に、例えば電源電位ＶＤＤに接続される１つのノード２２と、コード出力用の複数のノード２３_i（但し、ｉ＝１～ｎ、例えばｎ＝１００）を設けたものである。ノード２３_iの内の幾つかとノード２２の間は、導電性塗料を塗布して形成された固有の配線パター

ン２４によって、ランダムに接続されている。

【００２６】図３は、図２のＩＣカードの回路図である。このＩＣカードは、前述のコード発生部２０、ＩＣモジュール４０及びこれらの間を接続する信号線群３０を有している。コード発生部２０のノード２２は、電源電位ＶＤＤに接続され、各ノード２３ｉは、それぞれ信号線３１ｉを介して、ＩＣモジュール４０に接続されている。

【００２７】ＩＣモジュール４０は、各信号線３１ｉに対応するプルダウン用の抵抗４１ｉとバッファ４２ｉ、暗号部４３、データバス４４ａ，４４ｂ、機能部４５、記憶部４６及びアドレスバス４７を有している。

【００２８】バッファ４２ｉの出力側は、暗号部４３に接続されている。暗号部４３は、バッファ４２ｉから与えられる信号を暗号キーとして、データバス４４ａ上のデータを暗号化してデータバス４４ｂに出力すると共に、データバス４４ｂ上のデータを復号化してデータバス４４ａに出力するものである。

【００２９】データバス４４ａには、機能部４５が接続されている。機能部４５は、ＣＰＵ（中央処理装置）、ＲＯＭ（読出専用メモリ）、ＲＡＭ（随時読み書き可能なメモリ）及び入出力部等で構成され、入力部から入力された情報を、ＲＯＭに組み込まれたプログラムに従って処理するものである。

【００３０】データバス４４ｂには、記憶部４６が接続されている。記憶部４６は、ＥＥＰＲＯＭ（電気的に書き換え可能な不揮発性メモリ）等で構成され、機能部４５の処理結果である個人情報等のセキュリティを必要とする情報を格納するものである。

【００３１】アドレスバス４７は、機能部４５から記憶部４６に対して、読み書きのアドレスを指定するためのものである。

【００３２】次に、動作を説明する。コード発生部２０のノード２３ｉは、導電性塗料で形成された固有の配線パターン２４でランダムにノード２２に接続されているので、これらの各ノード２３ｉの電位は配線パターン２４の形状によって異なる。即ち、配線パターン２４で接続されているノード２３ｉは、電源電位ＶＤＤとなり、配線パターン２４で接続されていないノード２３ｉには、電圧が出力されない。

【００３３】各ノード２３ｉの電位は、それぞれ信号線３１ｉを介して、ＩＣモジュール４０内のバッファ４２ｉの入力側に導かれる。各バッファ４２ｉの入力側には、プルダウン用の抵抗４１ｉが接続されているので、配線パターン２４で接続されていないノード２３ｉに対応する信号線３１ｉは、接地電位ＧＮＤとなる。また、配線パターン２４に接続されたノード２３ｉに対応する信号線３１ｉは、電源電位ＶＤＤとなる。これらの信号線３１ｉの電位は、それぞれバッファ４２ｉを介して、暗号キーとして暗号部４３に与えられる。

【００３４】ここで、機能部４５から記憶部４６に対して書き込み動作が行われると、この機能部４５からアドレスバス４７を介して書き込み対象のアドレスが指定され、データバス４４ａ上に書き込むデータが出力される。データバス４４ａに出力されたデータは、暗号部４３によって暗号化されてデータバス４４ｂに出力される。そして、暗号化されたデータが記憶部４６に書き込まれる。

【００３５】次に、機能部４５から記憶部４６に対して読み出し動作が行われると、この機能部４５からアドレスバス４７を介して読み出し対象のアドレスが指定される。これにより、記憶部４６に格納されている暗号化されたデータが読み出され、データバス４４ｂ上に出力される。データバス４４ｂに出力されたデータは、暗号部４３によって復号化されてデータバス４４ａに出力される。そして、復号化されたデータが、機能部４５に読み取られる。暗号部４３に与えられる暗号キーは、コード発生部２０の配線パターン２４が変わらない限り変化しないので、機能部４５では書き込んだ通りのデータを読み出すことができる。

【００３６】一方、このＩＣカードを廃棄する場合には、図２（ａ）に示すように蓋１２を外し、窓部１１の内側にあるコード発生部２０の表面の配線パターン（導電性塗料）２４を、爪等で削り取る。これにより、配線パターン２４が変更され、暗号部４３に与えられる暗号キーが変化する。このため、機能部４５から記憶部４６に対して読み出し動作を行おうとすると、暗号キーが書き込み時から変化しているので、データを正しく読み出すことができない。

【００３７】以上のように、この第２の実施形態のＩＣカードは、導電性塗料による固有の配線パターン２４で暗号キーを発生するコード発生部２０を有すると共に、ＩＣカード本体１０に設けた蓋１２を外すことによって、このコード発生部２０の配線パターン２４を簡単に削り取ることができるようになっている。従って、廃棄時に容易に暗号キーを変え、記憶部４５の記録情報を読み出せなくしてセキュリティを確保することができる。

【００３８】また、コード発生部２０の配線パターン２４を削り取ったことを、目視で確認することができるので、安心してＩＣカードを廃棄することができるという利点がある。更に、ＩＣカード自体を破壊した訳ではないので、記憶部４６の記憶内容をすべて消去し、コード発生部２０の配線パターン２４を塗り替えれば、再利用することができるという利点がある。

【００３９】（第３の実施形態）図４は、本発明の第３の実施形態を示すＩＣカードの回路図であり、図３中の要素と共通の要素には共通の符号が付されている。

【００４０】このＩＣカードでは、図３中のＩＣモジュール４０に代えて、回路構成の異なるＩＣモジュール４０Ａを用いている。なお、本実施形態のＩＣカードの外

観は、図２（ａ）～（ｃ）に示した第２の実施形態のＩＣカードと同様である。

【００４１】ＩＣモジュール４０Ａは、コード発生部２０の各ノード２３ｉに接続された信号線３１ｉをプルダウンするための抵抗４１ｉ、コード設定部４８、一致検出部４９、機能部４５Ａ及び記憶部４６を有している。

【００４２】コード設定部４８は、このＩＣカードを特定するためのｎビットの識別コードを予め設定するもので、例えば、ｎ個のトランジスタの内、ゲートに選択的にイオンを注入してオン状態にしたトランジスタと、イオンを注入しないオフ状態のトランジスタの組み合わせによるマスクＲＯＭで構成されている。

【００４３】一致検出部４９は、コード発生部２０の各ノード２３ｉから信号線３１ｉを介して与えられる固有コードと、コード設定部４８に設定された識別コードを比較して、これらが一致したときに動作許可信号ＥＮを出力するものである。一致検出部４９は、コード発生部２０とコード設定部４８から与えられる対応する信号同士を比較するｎ個のＸＮＯＲ（排他的否定論理和ゲート）と、これらのＸＮＯＲの出力信号の論理積を動作許可信号ＥＮとして出力するＡＮＤ（論理積ゲート）とで構成されている。一致検出部４９の出力側は、機能部４５Ａのイネーブル端子に接続されている。

【００４４】機能部４５Ａは、ＣＰＵ、ＲＯＭ、ＲＡＭ、入出力部等で構成され、イネーブル端子に動作許可信号ＥＮが与えられたときに、入力部から入力された情報をＲＯＭに組み込まれたプログラムに従って処理するものである。機能部４５Ａには、システムバスを介してＥＥＰＲＯＭ等の記憶部４６が接続されている。

【００４５】このようなＩＣカードは、製造時に、ＩＣモジュール４０Ａのコード設定部４８にカード毎に固有の識別コードを設定し、コード発生部２０にはこの識別コード同じ固有コードを発生させるための配線パターン２４を導電性塗料で形成する。

【００４６】このようにして製造されたＩＣカードでは、コード発生部２０で発生された固有コードと、コード設定部４８に設定された識別コードが同一であるので、一致検出部４９から機能部４５Ａに対して動作許可信号ＥＮが出力される。これにより、機能部４５Ａによって所定の処理が行われ、処理結果の情報が記憶部４６に格納される。

【００４７】一方、このＩＣカードを廃棄する場合には、図２（ａ）に示すように蓋１２を外し、窓部１１の内側にあるコード発生部２０の表面を露出させる。そして、導電性塗料による配線パターン２４を、爪等で削り取る。これにより、配線パターン２４が変更され、一致検出部４９に与えられる固有コードが変化する。このため、一致検出部４９から機能部４５Ａに対する動作許可信号ＥＮが停止し、ＩＣカードの使用が不可能になる。

【００４８】以上のように、この第３の実施形態のＩＣカードは、導電性塗料による固有の配線パターン２４で、予め設定された識別コードと同じ固有コードを発生するコード発生部２０を有すると共に、ＩＣカード本体１０に設けた蓋１２を取ることによって、このコード発生部２０の配線パターン２４を簡単に削り取ることができるようになっている。従って、廃棄時に容易に固有コードを変え、ＩＣカード自体を使用不可能な状態にすることができ、記憶部４６の記録情報を読み出せなくしてセキュリティを確保することができる。

【００４９】また、コード発生部２０の配線パターン２４を削り取ったことを、目視で確認することができるので、安心してＩＣカードを廃棄することができるという利点がある。

【００５０】なお、本発明は、上記実施形態に限定されず、種々の変形が可能である。この変形例としては、例えば、次のようなものがある。

【００５１】（ａ）　図１のＩＣカードでは、廃棄時にＩＣモジュール３を確実かつ容易に破壊するために、三角溝１ｂを設けているが、矩形や半円形の溝でも良い。

【００５２】（ｂ）　図１中の補強材５は、ＩＣカード表面の一部にだけ貼り付けているが、このＩＣカード全面に貼り付けても良い。これにより、表面が平らに仕上がり、操作性及び体裁が良くなる。

【００５３】（ｃ）　図２のＩＣカードでは、製造時に、予め固有の配線パターン２４を形成して個々の暗号キーを発生させるようにしてから、ＩＣカード本体１０に埋め込み、更に窓部１１を蓋１２で閉じて完成したＩＣカードとしている。しかし、製造時に、コード発生部２０のノード２２をすべてのノード２３ｉに接続する配線パターン２４を形成しておき、ユーザが使用開始の直前に配線パターン２４の一部を削って固有の暗号キーを発生させるようにしても良い。これにより、廃棄後に暗号キーを知ることが一層困難になり、セキュリティを保護することができる。この場合、製造時には、窓部１１に蓋１２を仮り止めしておき、ユーザが固有の暗号キーを設定した時点で、蓋１２を固定するようにする必要がある。

【００５４】（ｄ）　図３及び図４において、コード発生部２０のノード２２を電源電位ＶＤＤに接続しているが、このノード２２を接地電位ＧＮＤに接続しても良い。その場合、抵抗４１ｉはプルアップ抵抗として一端を電源電位ＶＤＤに接続する必要がある。

【００５５】

【発明の効果】以上詳細に説明したように、第１の発明によれば、ＩＣモジュールの埋め込み箇所のカード表面に溝を設け、この溝を覆うように補強用のプラスチック板を粘着材で貼り付けている。従って、プラスチック板により通常の使用状態での強度が保たれ、廃棄時には、プラスチック板を剥がして溝の部分でカード本体を折り曲げることにより、ＩＣモジュールを確実に破壊するこ

とができる。これにより、廃棄時のセキュリティを容易に確保することができる。

【００５６】第２の発明によれば、導電性塗料による配線パターンで暗号キーを発生するコード発生部と、この暗号キーを使用して機能部と記憶部の間のデータを暗号化する暗号部を有している。従って、廃棄時に配線パターンを削り取れば暗号キーが変更され、記憶部に格納されたデータを正しく読み出すことができなくなる。これにより、廃棄時のセキュリティを容易に確保することができる。

【００５７】第３の発明によれば、導電性塗料による配線パターンで固有コードを発生するコード発生部と、この固有コードが予め設定された識別コードと一致したときに動作許可信号を出力する一致検出部を有している。従って、廃棄時に配線パターンを削り取れば固有コードが変更され、動作許可信号が停止して機能部の処理が不可能になる。これにより、廃棄時のセキュリティを容易に確保することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示すＩＣカードの概略の構成図である。

【図２】本発明の第２の実施形態を示すＩＣカードの概略の構成図である。

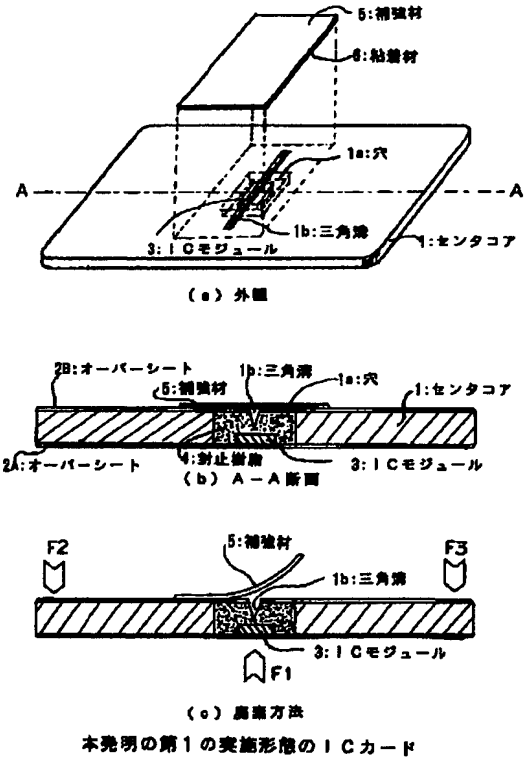
【図３】図２のＩＣカードの回路図である。

【図４】本発明の第３の実施形態を示すＩＣカードの回＊路図である。

【符号の説明】

１　センタコア
２Ａ，２Ｂ　オーバーシート
３，４０，４０Ａ　ＩＣモジュール
４　封止樹脂
５　補強材
６　粘着材
１０　ＩＣカード本体
１１　窓部
１２　蓋
２０　コード発生部
２２，２３　ノード
２４　配線パターン
３１　信号線
４１　抵抗
４２　バッファ
４３　暗号部
４４ａ，４４ｂ　データバス
４５，４５Ａ　機能部
４６　記憶部
４７　アドレスバス
４８　コード設定部
４９　一致検出部

【図１】



本発明の第１の実施形態のＩＣカード

【図３】

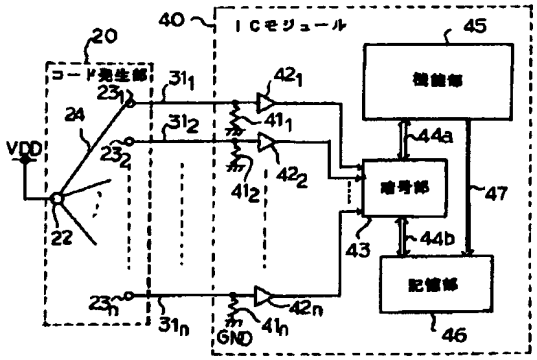
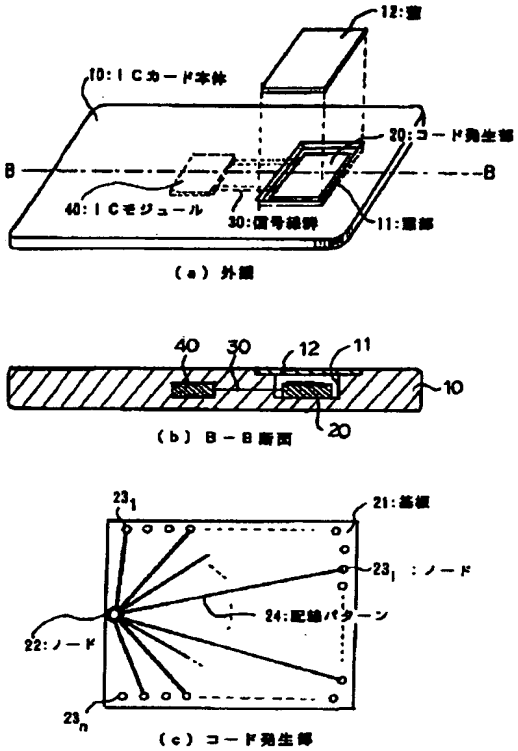


図２のＩＣカードの回路

【図２】



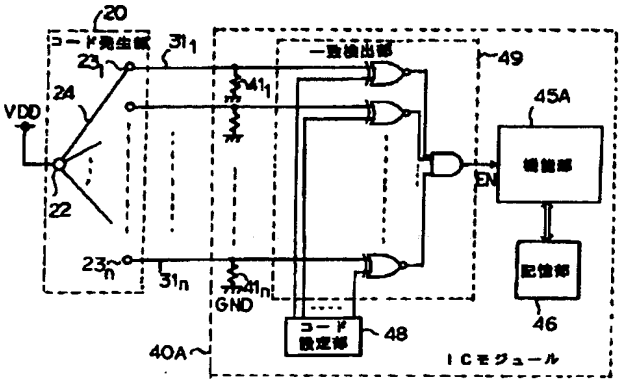
（ａ）外観

（ｂ）Ｂ－Ｂ断面

（ｃ）コード発生部

本発明の第２の実施形態のＩＣカード

【図４】



本発明の第３の実施形態のＩＣカードの回路